RSAC 2025 Conference

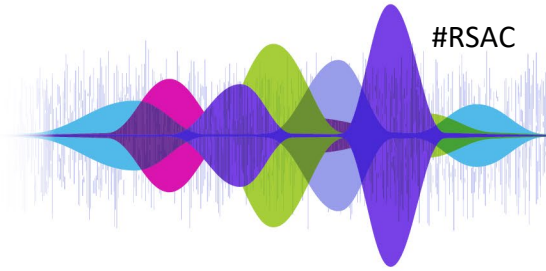
Many Voices.
One Community.

SESSION ID: NCS-R02

Layering Threat Models to Drive Zero Trust Policies and Solutions

Brenna Leath

Software Security Principal
Navy Federal Credit Union
Linkedin.com/in/brennaleath



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

All images in this session used with permission from Microsoft Stock Image, 2024, unless credited under Creative Commons, Fair User provisions of the United States Copyright Act, or otherwise.

Portions of “Map the Transaction Flows” are quoted and attributed to the Cloud Security Alliance, accessible at *https://cloudsecurityalliance.org.*

Agenda

#RSAC

Understand Your Attack Surface

…Then Protect the Surface

Definitions and Options

Designing the Design

Templates and Layers

Challenges

Apply!

RSAC™ 2025 Conference

Understand Your Attack Surface

…Then, Protect the Surface

Many Voices.
One Community.

NIST.SP.800-207: Pathway to Implementing a ZTA

True or False?

"The First Step is Always an Asset Inventory"

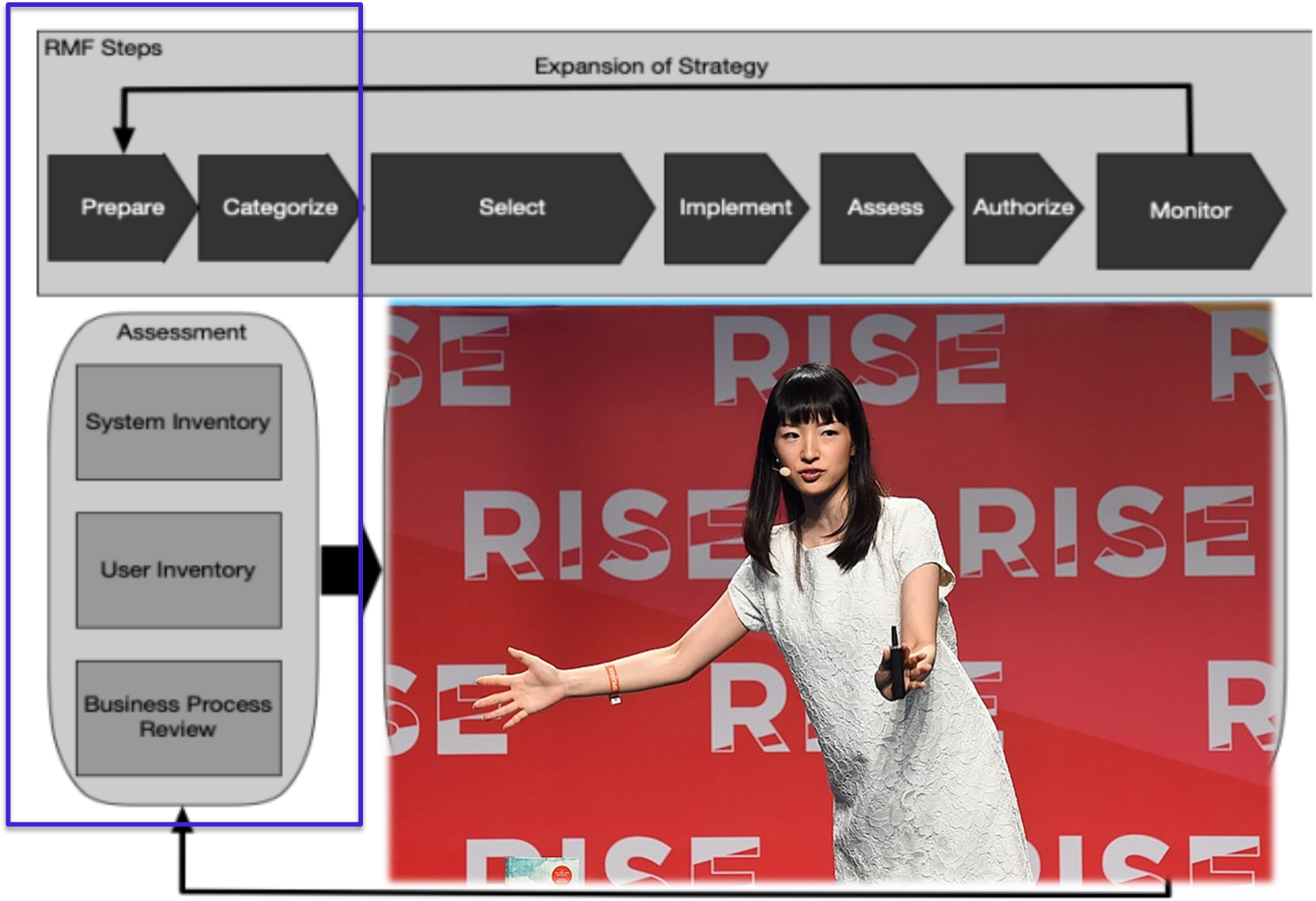


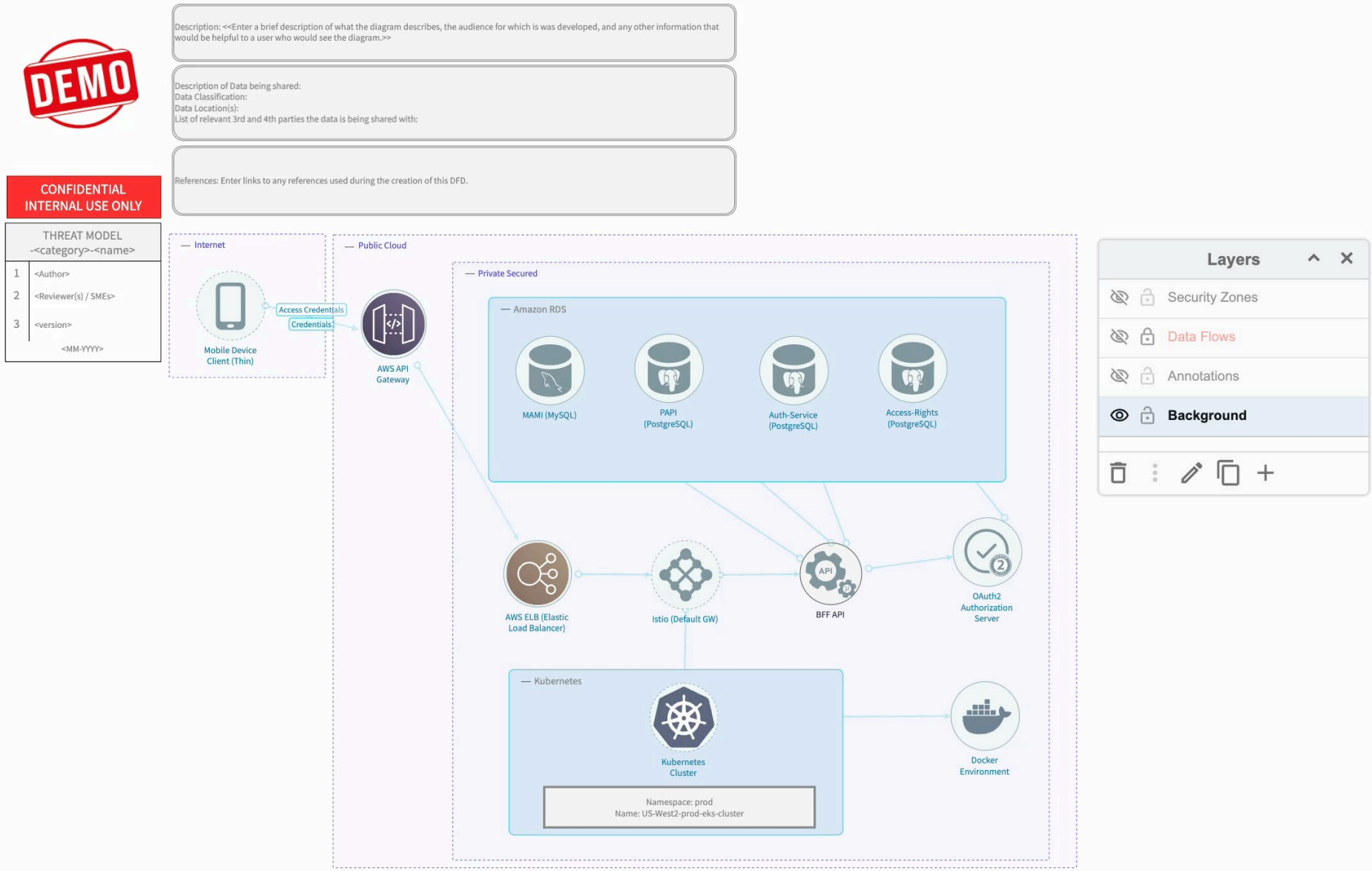
Figure 12: ZTA Deployment Cycle

Rule 1: Commit ~~Yourself~~ to Tidying Up Your Leadership

"Hans Solo" by AZRainman is licensed under CC BY 2.0.
"Darth Grader" by JD Hancock is licensed under CC BY 2.0.

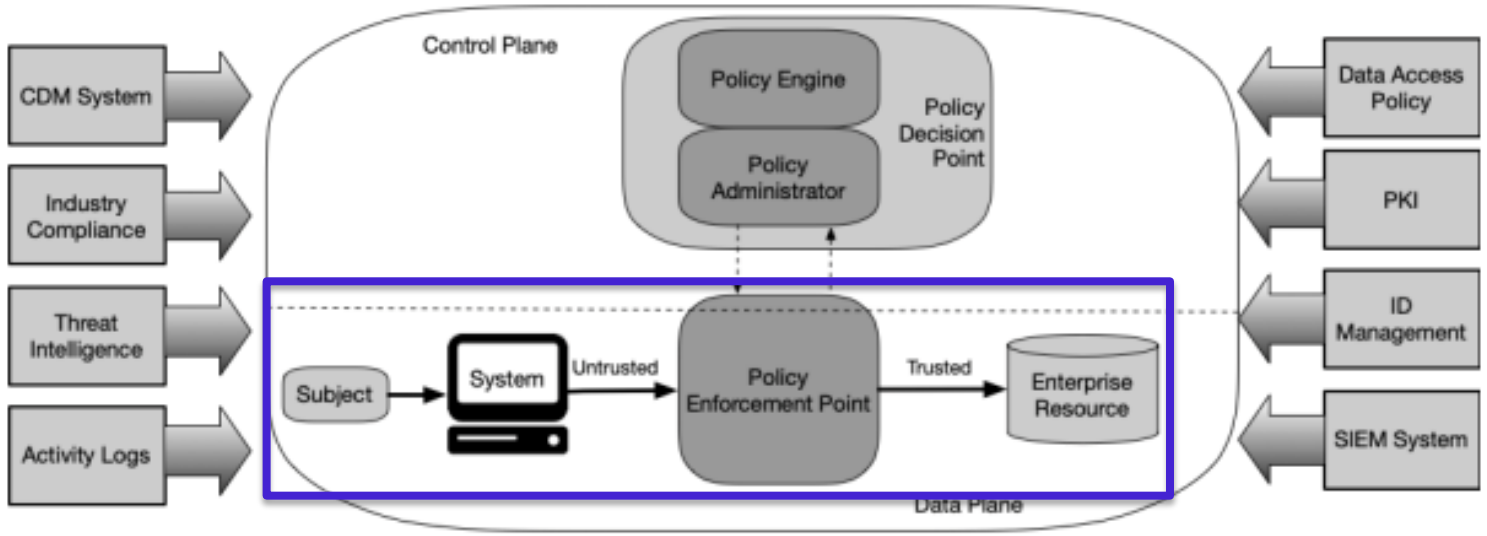
Rule 2: Imagine Your ~~Ideal Lifestyle~~ Future-State Zero Trust Architecture

Rule 2: Imagine Your Ideal ~~Lifestyle~~ Diagram



Frameworks, Tenets, Principles, Capabilities

NIST.SP.800-207: Core Zero Trust Logical Components



NIST SP 800-207
DoD Zero Trust Overlays
CSA Zero Trust Framework
…Gartner Zero Trust for Dummies

- Data Discovery and Classification
- Asset Discovery and Attack
- Configuration and Patch Management
- Identity and Access Management
- Third Party Risk Management
- Micro-Segmentation
- Context-based Access Control
- Least Privilege Access
- Encryption and Data Protection
- Security Monitoring and Logging

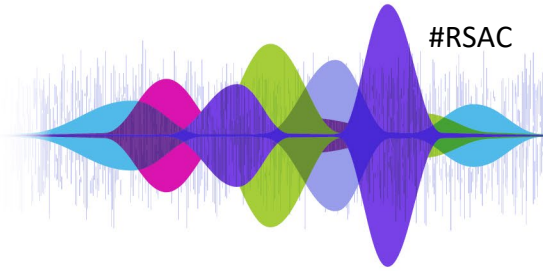
Rule 3: Finish Discarding First

"We should be choosing what we want to keep, not what we want to get rid of."

-Marie Kondo

Align with the business to what is **in-scope**

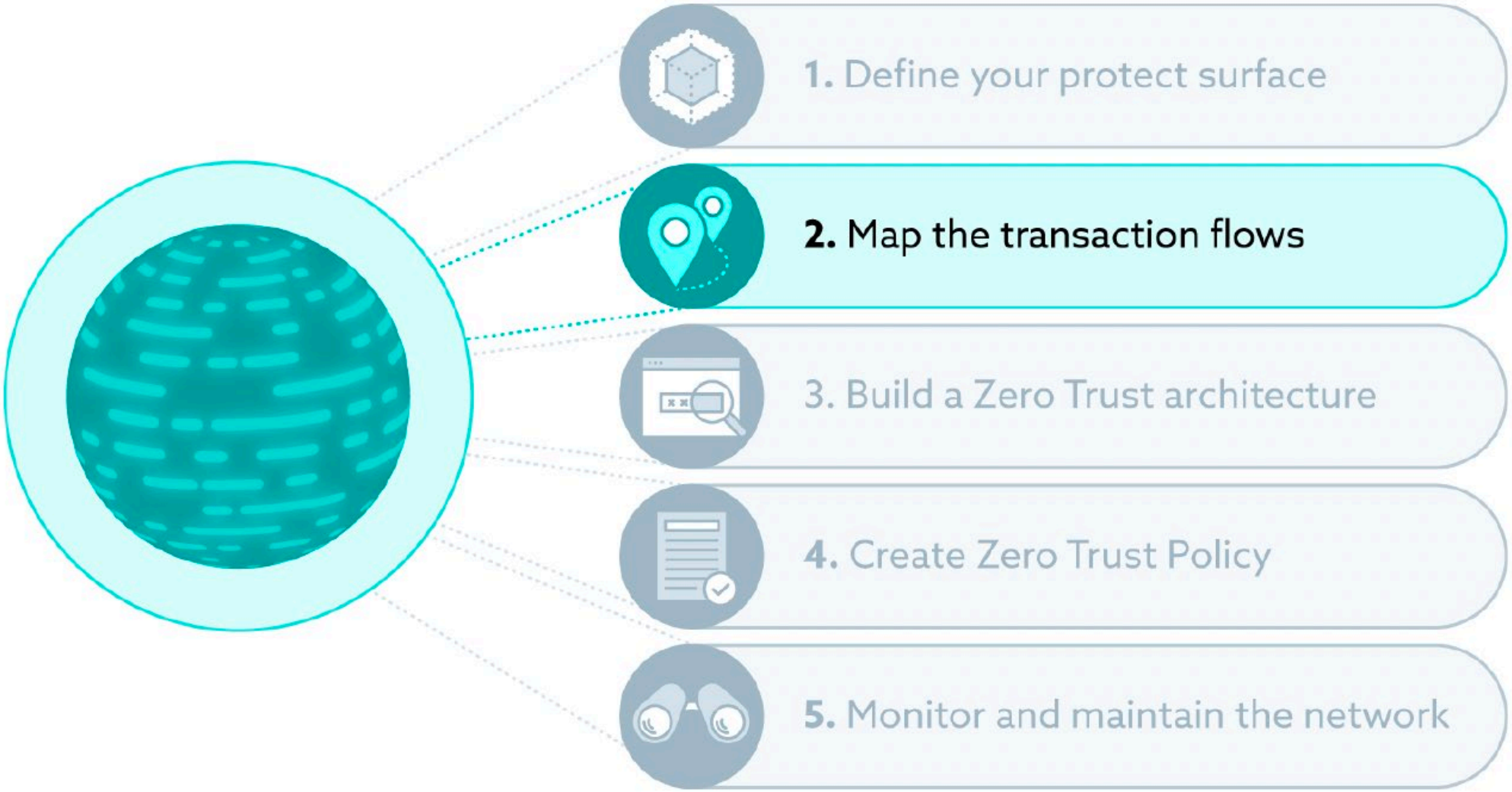
- Legacy Debt, Technical Debt
- Cloud Migration and Consolidation
- Application Rationalization



Example Eligibility Criteria

Eligible	Ineligible
• Enterprise platforms that are the secure-by-design paved roads where ZT controls will be concentrated • 1st and 3rd party business applications processing or storing data classified as restricted • Mobile applications	• Applications smaller than (x) lines of code / (x) number of components • Applications in reduced maintenance mode (scheduled decommission within (x) time) • Applications where primary risks are inherited from transitive dependencies (apps, libraries, etc) upon which controls will be focused • Isolated single servers running a process or batch job with no UI

CSA 5-Step Process for Zero Trust Implementation


1. Define your protect surface
2. Map the transaction flows
3. Build a Zero Trust architecture
4. Create Zero Trust Policy
5. Monitor and maintain the network

© Copyright 2024, Cloud Security Alliance. All rights reserved.

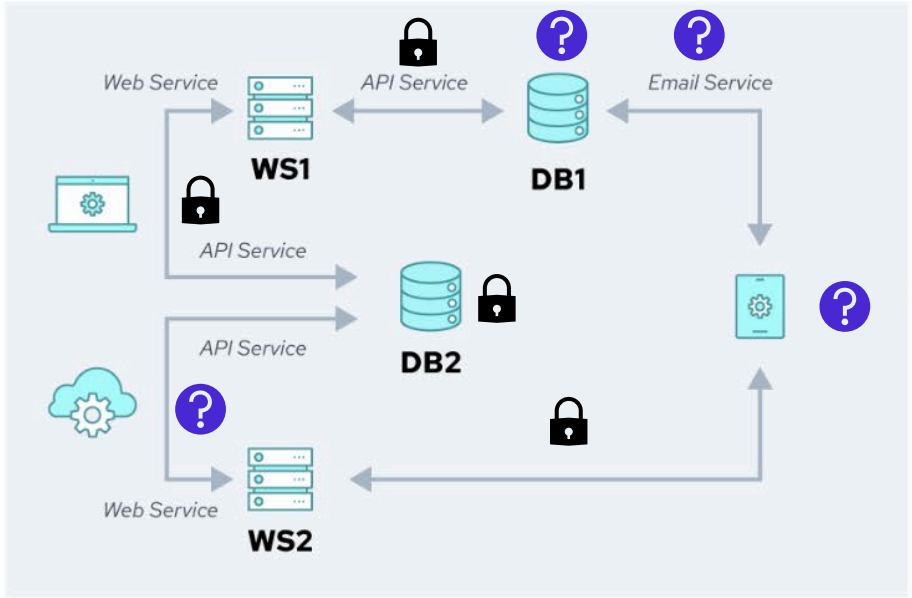
RSAC 2025 Conference

Definitions and Options

Define → Map → Refine → Protect

Defined Protect Surfaces

Transaction Flow Mapping



Refined Protect Surfaces

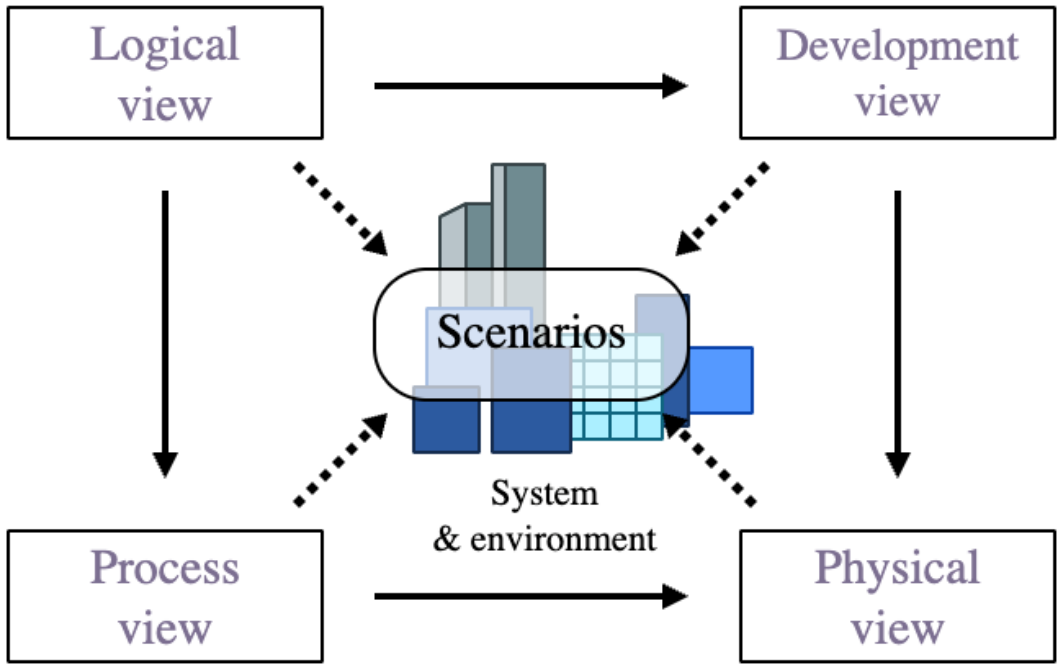
- Micro-Segmentation
- Context-based Access Control
- Least Privilege Access
- Encryption and Data Protection
- Security Monitoring and Logging

© Copyright 2024, Cloud Security Alliance. All rights reserved.

Rule 4: Tidy by Category, Not by Location

"By bringing all similar items together, you can accurately see the total picture, which helps in making informed decisions."

- **Data flow diagrams (DFDs)** are graphical representations of how data moves through a system, using symbols to show data flows, data stores, data processes, and data sources.
- **A threat model** is a structured way to identify, assess, and reduce potential security risks. It's a type of risk assessment that helps organizations understand how threats could impact their systems and networks.
- **A zero trust data flow diagram (ZT DFD)** is DFD created to meet ZTA MVP requirements, created independently of and potentially reusable by any other DFD procedure.



Leverage Observability, Scanning, and Monitoring Tools

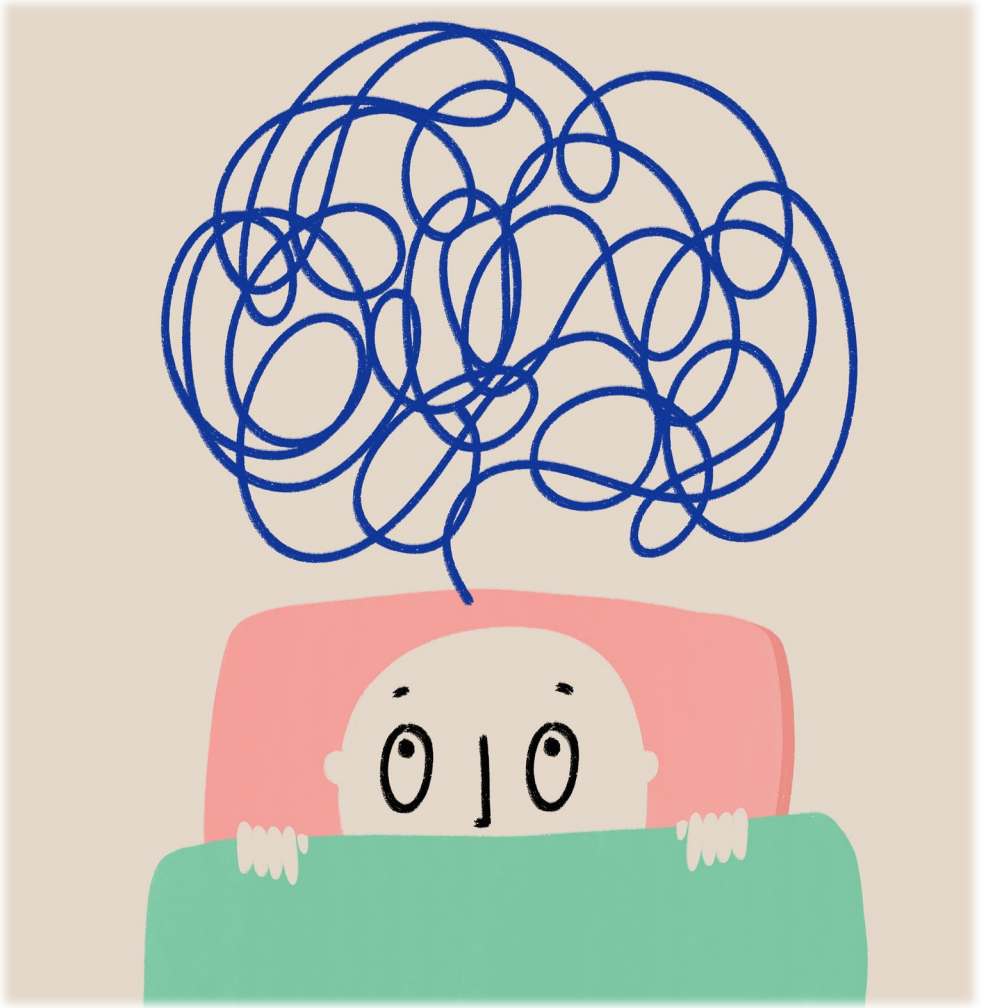
Tool types	Purpose	Data	Usage
Application Observability and Analysis Tools (Example: Jaeger, Fluentd, Prometheus, OpenTelemetry)	These tools can understand the system from its external outputs.	1. Tracing data 2. Performance Metrics	Observability tools collect telemetry data that is consumed by analysis tools, which aid in querying or visualizing the data
Log Analysis Tools (Example: Splunk, ELK Stack, Sumo Logic)	These tools collect, centralize, and analyze log data from applications, servers, and network devices.	1. User activities (Authentication, access requests, data modifications) 2. Log events (App logs, server logs, security logs)	Help identify application errors, exceptions, and issues.
API Monitoring Tools (Example: Postman, Apigee, Kong, Layer7 API gateway)	These tools track and monitor interactions between applications, APIs, microservices, and external systems.	1. API calls (request, response, headers, parameters) 2. API status 3. Usage analytics (API usage patterns, API traffic)	It helps monitor API availability, track API usage, and identify API usage trends.
Network Monitoring Tools (Example: Wireshark, Nagios, SolarWinds Network, Service Mesh tools, Service Proxy tools, Identity Aware Proxies, Performance Monitoring tools)	They capture and analyze network traffic, including application-level protocols, to monitor system interactions and data exchanges.	1. Network traffic data (packet headers, payloads, protocols) 2. Network device status 3. Service-level communication (HTTP, FTP, SMTP, etc.)	It helps visualize network traffic flows, identify system communication patterns, and monitor service availability.
Database Monitoring Tools (Example: SolarWinds Database Performance Analyzer, Oracle Enterprise Manager, SQL Sentry)	These tools monitor database performance, query execution, and data access patterns to capture interactions with database systems.	1. Database server logs and events 2. Performance metrics 3. Session information	It helps analyze database transactions, data access patterns, and resource utilization
Application/Transaction Monitoring Tools (Example: Dynatrace Transaction Monitoring, AppDynamics Business iQ, Service Mesh)	They track end-to-end transactional workflows, identify transaction paths, and monitor transaction performance.	1. Transaction traces 2. Business transaction data (user actions, system interactions) 3. Transaction performance metrics	It helps to analyze user interactions and the business impact of transactional activities

© Copyright 2024, Cloud Security Alliance. All rights reserved.

What Are Your Options?

…and, what are your problem statements?

- "We have different teams making diagrams, but **the diagrams are inconsistent, confusing, or incomplete**."
- "We have parts of this information scattered all over the place. Now the application team is already frustrated at being derailed by 'Security' projects because **the team repeats themselves** to different security and compliance teams at multiple touchpoints in the SDLC."
- "We have no diagrams at all! It's **CHAOS**!"



CATEGORIZE: DISTILL MVP CRITERIA

SIMPLIFY: TECHNOLOGY CAPTURES, TEMPLATES, + JOB AIDS

BRING IT TOGETHER: USE LAYERS TO CUSTOMIZE VIEWS

RSAC™ 2025 Conference

Designing the Design

Rule 5: Follow the Right Order

CSA Transaction Flow Mapping Process

API Specifications

Design Artifacts

Flowcharts and Process Diagrams

Transaction Flow Mapping

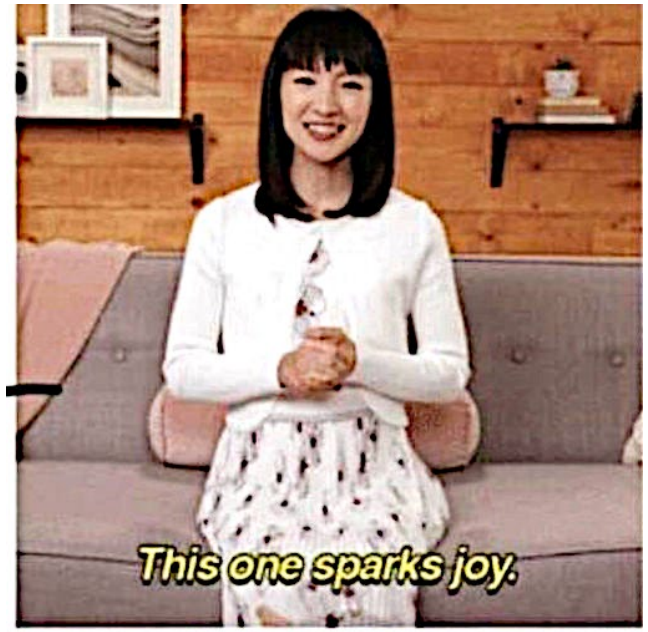
Identify Entry Points and Data Payloads

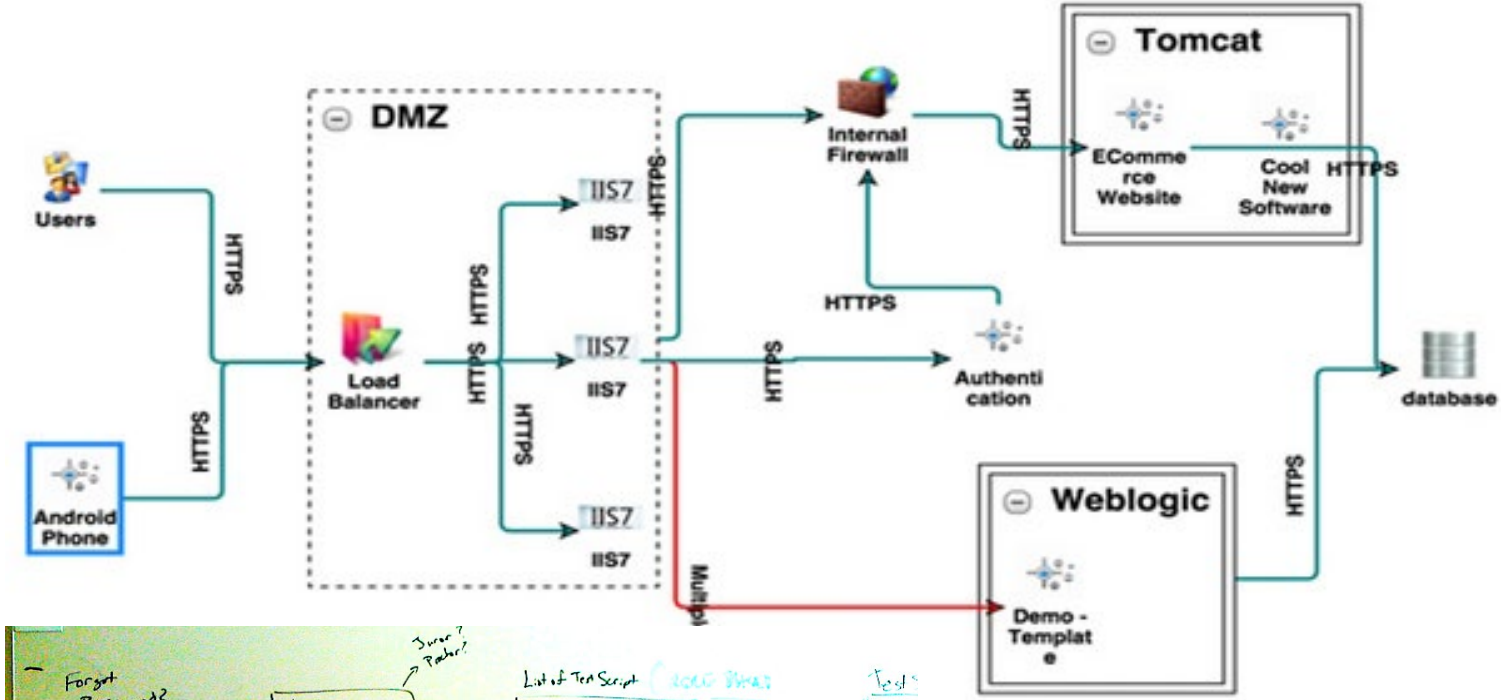
Understand Component Interactions

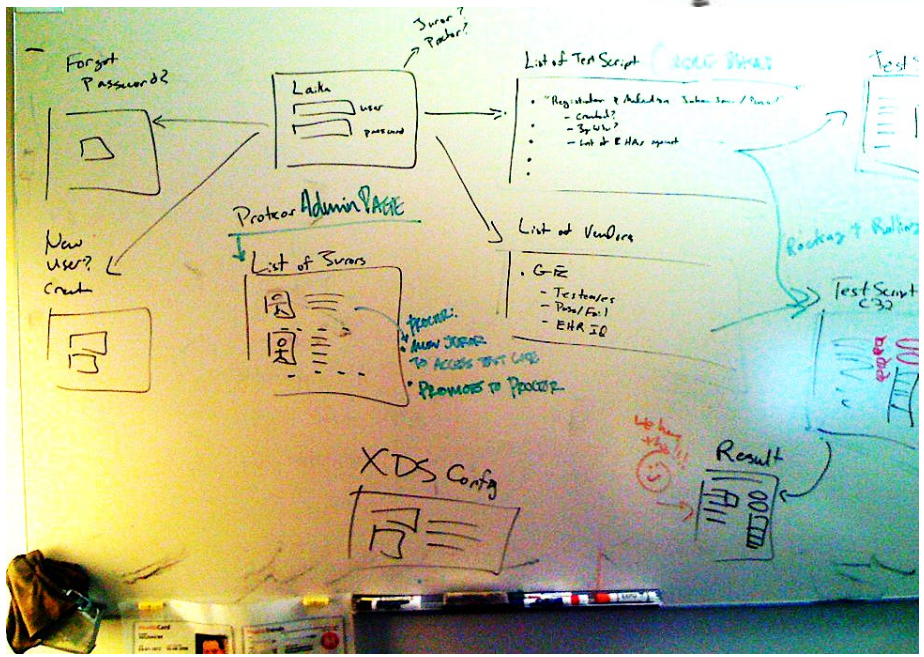
Assess Security Controls

Comprehensive Understanding of Transaction Flows

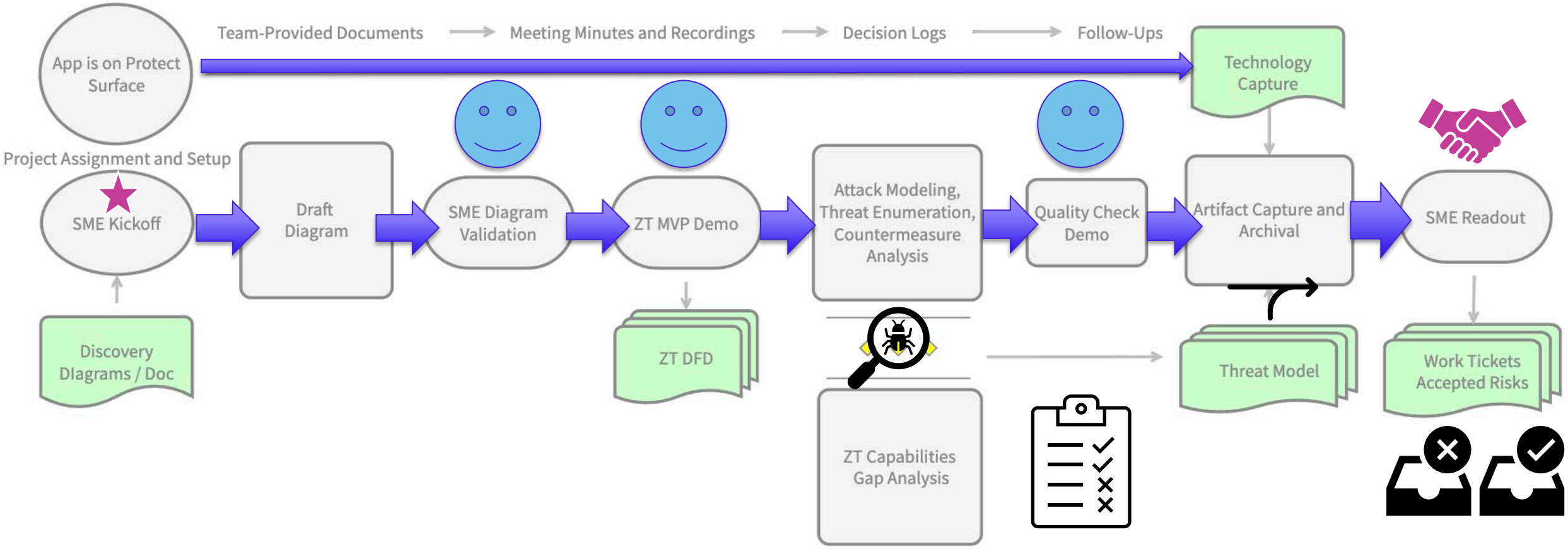
Rule 6: Ask Yourself If It Sparks Joy







Rule 5: Follow the Right Order



Step-by-Step

1. Identify stakeholders who can a.) partner to get and give information b.) derive value from your downstream work products.
2. Distill zero trust minimal viable product (ZT MVP) criteria.
3. Devise templates for consistency of capture.
    1. Technology Capture & Job Aids
    2. Threat Model Template
4. Use layers to allow downstream consumers to customize views.
    1. Layer 1: Background – Infrastructure, Network, Components, Flows
    2. Layer 2: Annotations – Assets, Security Controls, Threat Actors
    3. Layer 3: Data Flows – “Data Connection Stories”
    4. Layer 4: Network Security Zones – High Risk, Low Risk

1. Identify Stakeholders

- Security teams:
  - Inputs for microsegmentation and ‘Just-in-Time’ RBAC zero trust solutioning efforts
- Threat analysis team:
  - Brief pen testers on suspected weaknesses during recon
- Enterprise architecture teams
  - supplement or replace team data flow diagrams

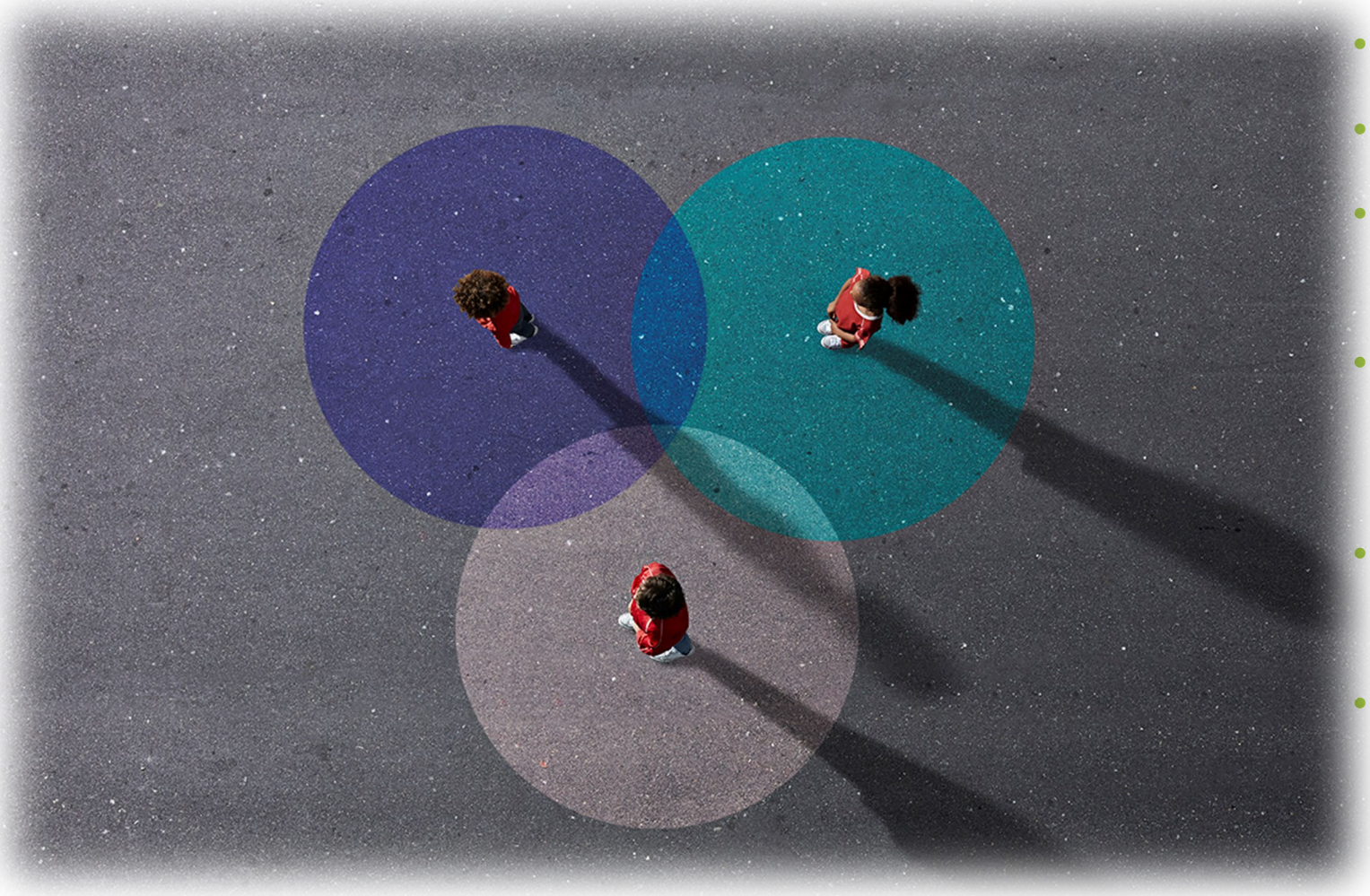
Other consumers might be:

- Adjacent dev teams
- QA
- Network / cloud
- Compliance / GRC

Establish the contexts and rules for re-use

- “need-to-know” repository

2. Distill MVP Criteria



- Description of data being shared
- Data classifications, storage, and location(s)
- Relevant 3rd and 4th parties sharing data
  - (Layer 1: Background)
- Description of information security controls implemented
  - (Layer 2: Annotations)
- Data flows & threat actor attack paths
  - (Layer 3: Data Flows)
- Overlay of any network security zones corresponding to logical security network architecture.
  - (Layer 4: Security Zones)

3. Template a “Technology Capture”

Technology Capture:
Metadata, Context, Tribal Knowledge
(.doc, Wiki, central DB, knowledgebase)

- SMEs
- Scope of the model
- Technologies and stacks
- Source code (languages, repositories)
- Roles, permissions, IdPs
- Preventative / administrative controls
- Inputs, outputs
- Assumptions and decisions

Job Aids:
Enable Consistency & Handoffs
(.ppt, .doc, Wiki, issue trackers)

- Kickoff deck templates
- Meeting agenda templates
- Custom diagram templates
- Finding tracker / ticket templates

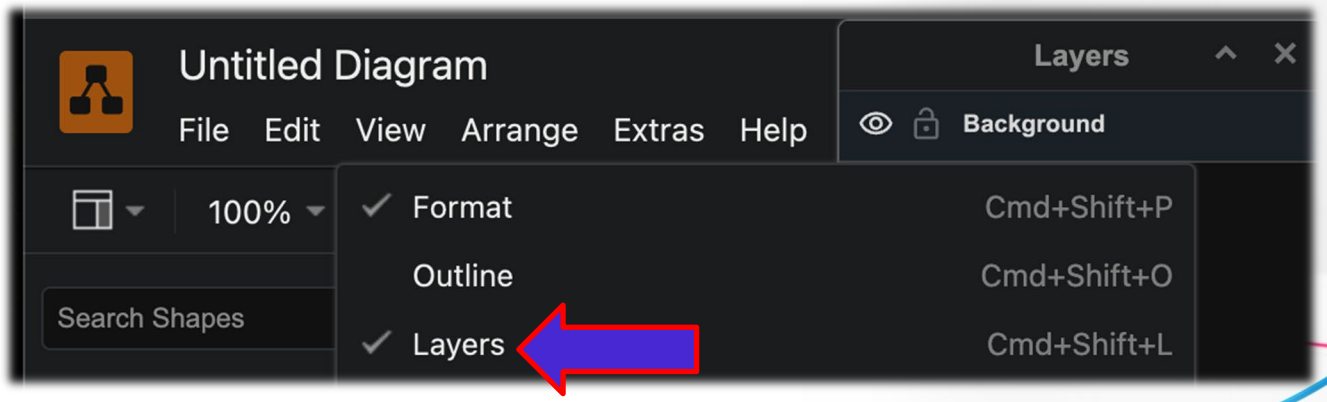
4. Use Layers to Customize Views

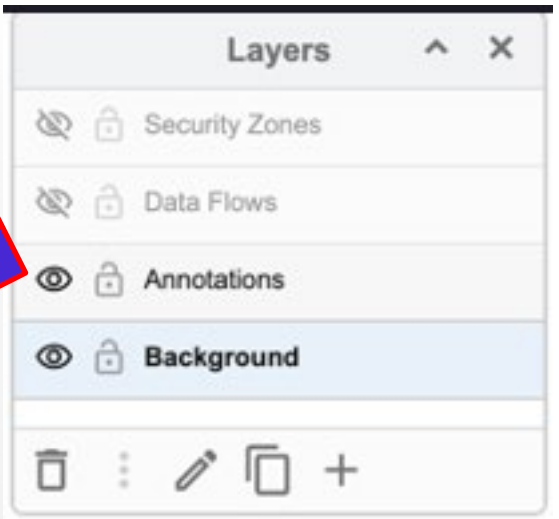
Benefits to Creators

- Define layers based on how each consumer needs data captured and presented
- Scalable approach: New team? New layer!

Benefits to Viewers

- Reuse diagram while reducing complexity
- Show/hide data as they like
- Can be output as individual files tailored to each team

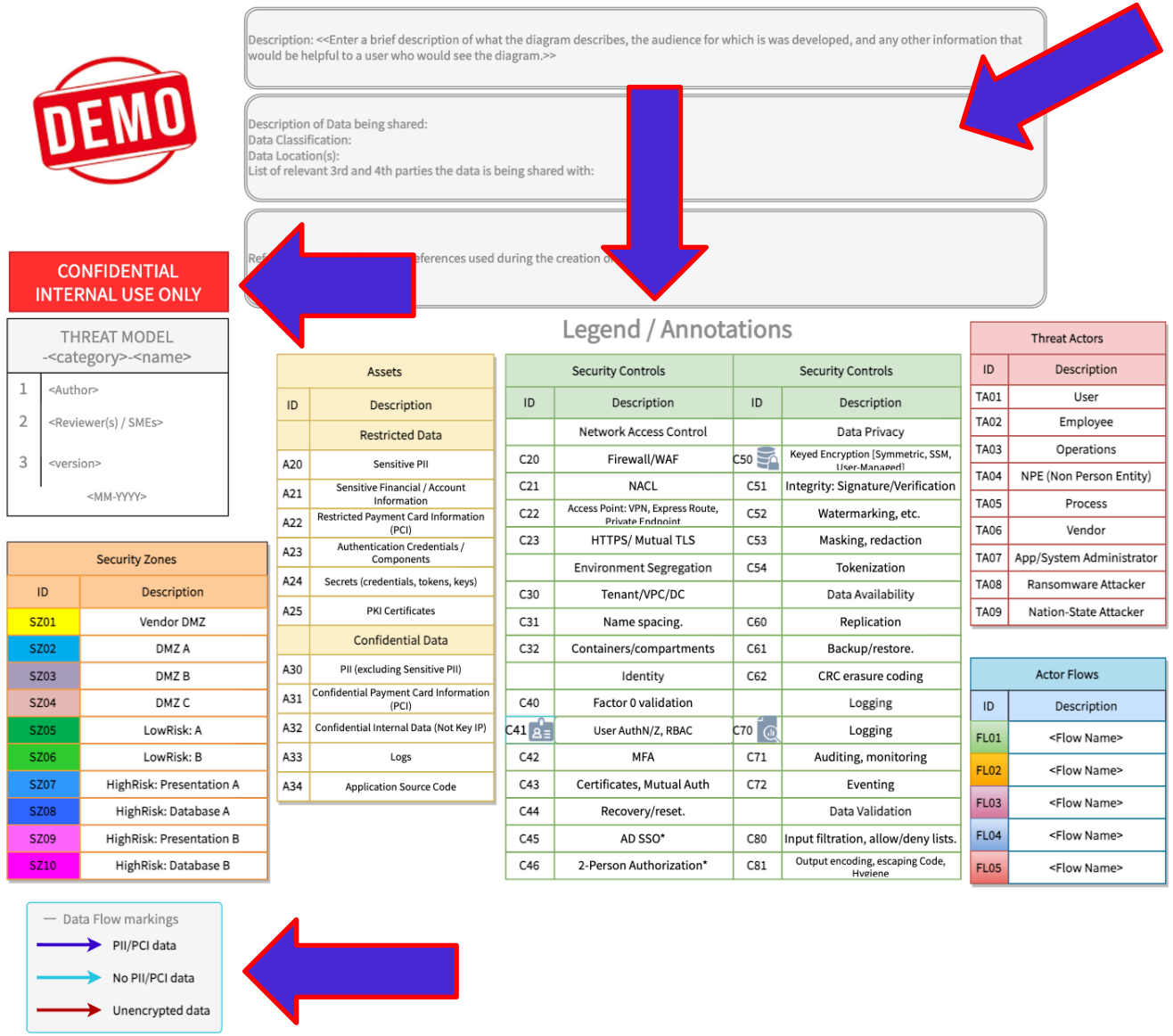




RSAC™ 2025 Conference

Templates and Layers

Elements of a ZT DFD Template



Key elements:

- Standard metadata capture
- Data classification labeling for DLP
- Tables for annotations
- Legend for color coding

Layer 1: Background

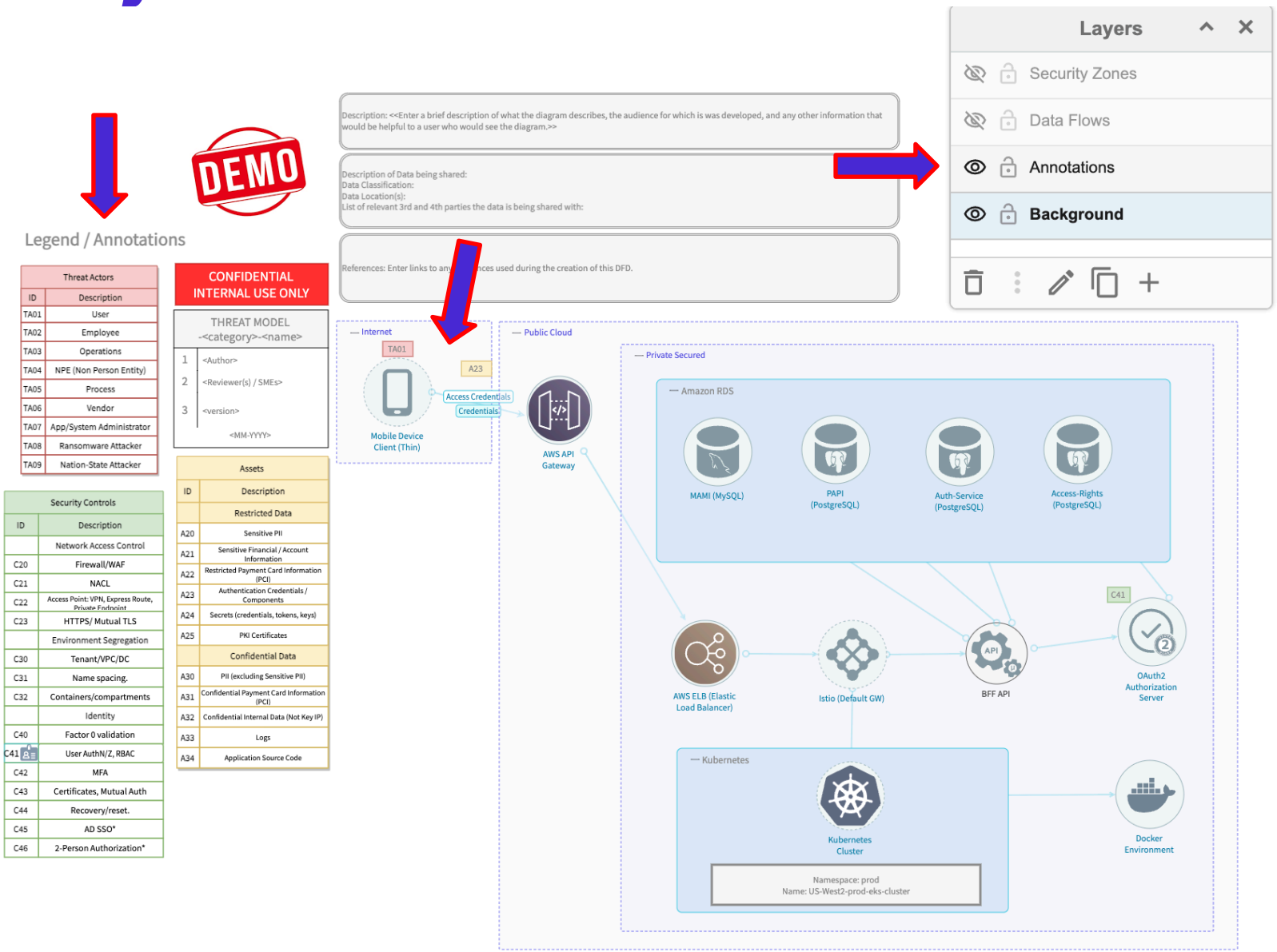
Key elements:

- Metadata
- Trust zones & trust boundaries
- Diagram components
- Data flows and data tags

Useful for:

- Everybody ☺

Layer 2: Annotations



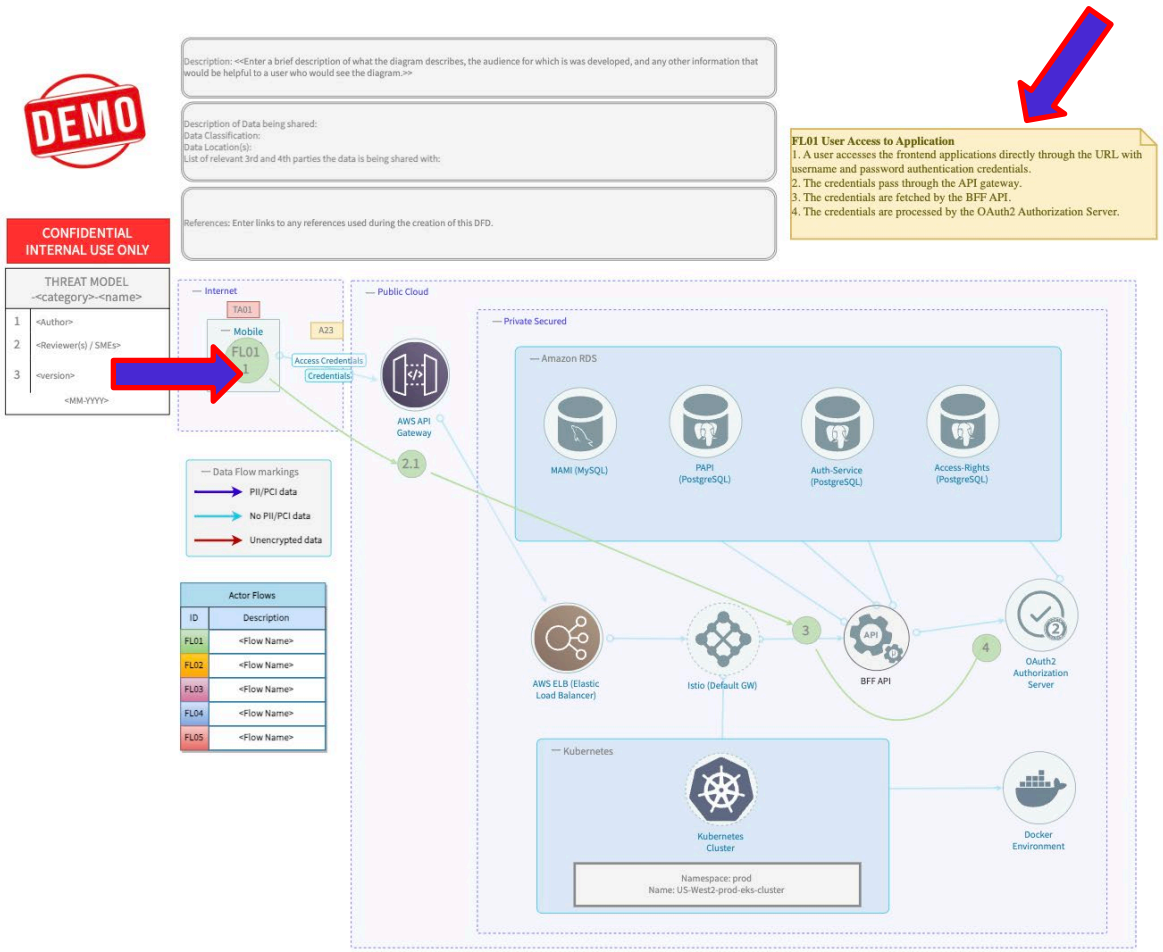
Key elements

- Security controls
- Threat actors
- Labels
- Notes as needed

Useful for:

- Security teams, pen testers
- Solutioning teams
- Development teams

Layer 3: Data Flows



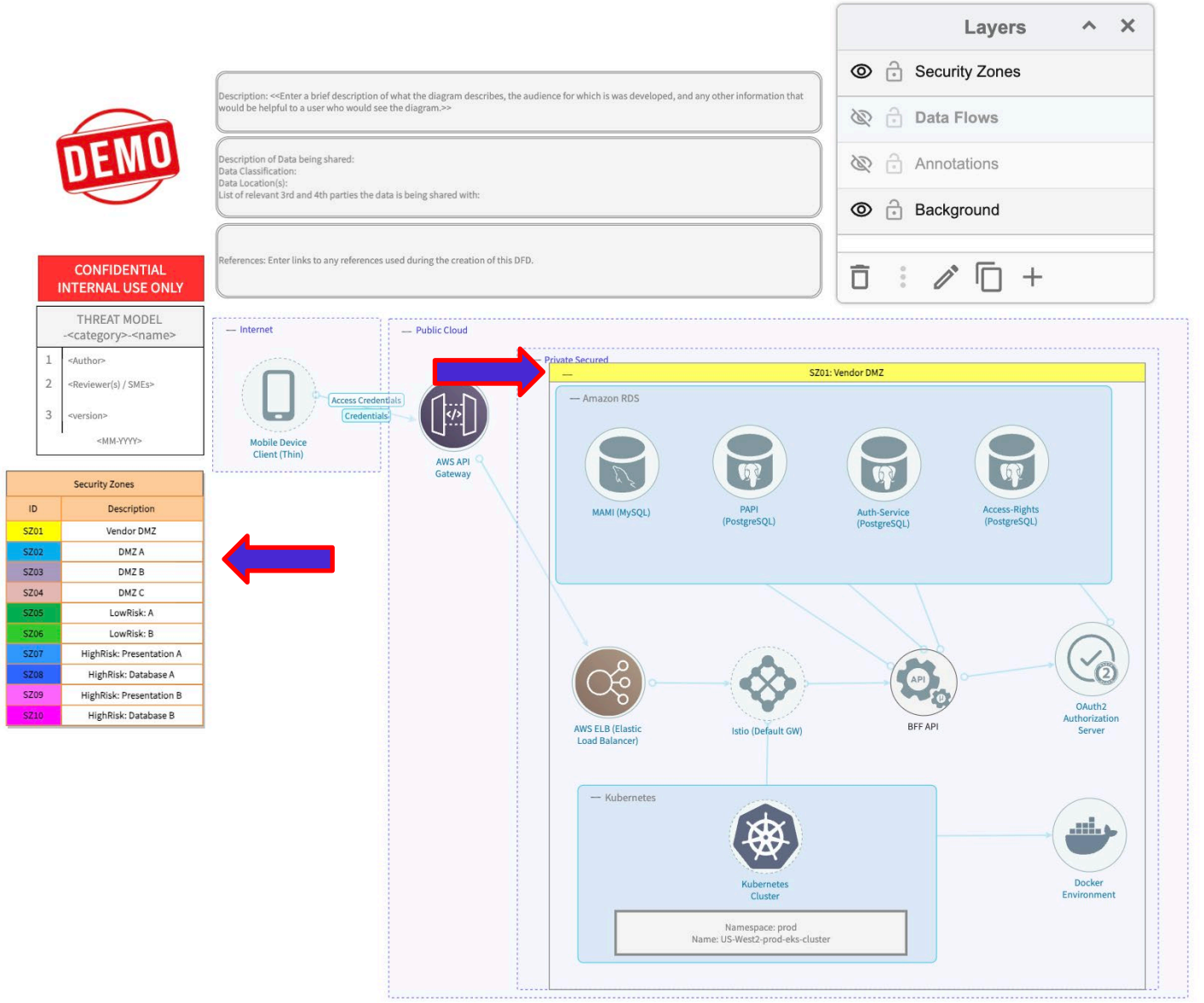
Key elements

- Numbered data flows by threat actor
- Notes describing actor actions

Useful for:

- Architecture teams
- Solutioning teams
- Pen testers

Layer 4: Security Zones



- Key elements
  - Network zones tagged by risk

Useful for:

- Security teams
- Solutioning teams
- Network teams

RSAC 2025 Conference

Challenges

Challenges

No “one size fits all”

- Varying fidelity of inputs, availability of resources
- Balance between depth of detail and velocity

Complex lexicon

- Color coding
- Custom components
- Icons

Tooling differences & challenges

- Not all tools support total functionality of layers
  - Tags in draw.io vs. layers
- Different teams use different diagramming tools
- Sometimes ‘re-dos’ are inevitable

RSAC™ 2025 Conference

Time to Tidy!

Summary

The 6 Rules of Tidying Up	…to Tidy Up Your Transaction Flows
Rule 1: Commit Yourself to Tidying Up	Executive Sponsorship Project Charter
Rule 2: Imagine Your Ideal Lifestyle	Define the Protect Surface Understand the Attack Surface Prioritize ZT Capabilities
Rule 3: Finish Discarding First	Establish Eligibility Criteria
Rule 4: Tidy by Category, Not by Location	Discovery and Technology Capture Synthesize Resources
Rule 5: Follow the Right Order	Design Your Process
Rule 6: Ask Yourself if it Sparks Joy	Design Your Templates Design Your Layers

Apply!

- **Next Week: Use Technology Captures** to help downstream consumers retrace your steps and quicken comprehension of the system design.
  - These can be as simple as a collection of meeting notes and recordings. What data are you gathering that other people could re-use at a later stage in the SDLC?
- **In 3 Months: Layer Architecture Diagrams** to allow other teams in your ecosystem to customize perspectives.
  - What layers could you add to make your threat model a useful input to your peers and speed their time-to-value?
- **In 6 Months: Use a 'Weighted' Approach** – what you capture for your models can vary in weight depending on the inherent risk and complexity of the subject.

  T-shirt-size the varying value to be gained from…
  - A whiteboard of a new feature threat modeled by an engineer
  - A new application integration threat modeled by a security architect
  - A full system cloud migration threat modeled by a principal cloud security architect
- **Spring Cleaning:** An iterative threat modeling process enhanced by automation can keep your ZT DFDs fresh, evolving and improving continuously.

RSAC 2025 Conference

Many Voices.
One Community.

Thank You

For More Information:

https://cloudsecurityalliance.org/

https://www.threatmodelingconnect.com/

Draw.io